UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/529,346	03/25/2005	Kalle Ahmavaara	39700-766N01US/NC39614US	6681

64046 7590 08/14/2009
MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C
ONE FINANCIAL CENTER
BOSTON, MA 02111

EXAMINER	
BALAOING, ARIEL A	
ART UNIT	**PAPER NUMBER**
2617	
MAIL DATE	**DELIVERY MODE**
08/14/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)	
Office Action Summary	10/529,346	AHMAVAARA ET AL.	
	Examiner	**Art Unit**	
	ARIEL BALAOING	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,12-16,19-24,26-38 and 41-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,12-16,19-24,26-38 and 41-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/20/2009 has been entered.

Response to Arguments

2. Applicant's arguments filed 05/08/2009 have been fully considered but they are not persuasive.

Regarding the applicant's arguments that:

"*Claims 30 and 32-34 were rejected under 35 U.S.C. 112, first paragraph, as allegedly failing to comply with the written description requirement. In particular, the Office Action asserted that the limitation a "computer-readable storage medium having computer-executable components" is not included in the specification. Applicants have amended claims 30 and 32-34 to recite a "computer-readable storage medium encode with instructions configured to control a processor to perform a process" or a "data structure embodied on a computer-readable medium." Support for these amendments may be found in the specification, for example, at page 7, lines 18-33, which discloses client software at an user equipment (UE), and at Figure I, which discloses an authentication server 50 allocated with an authentication server database 55. One of* *ordinary skill in the art would appreciate that the authentication server is typically equipped with a "computer-readable storage medium," for example, a memory, and that the authentication server database may correspond to the "computer-readable storage medium." Accordingly, Applicants respectfully submit that this rejection is moot in view of the claim amendments, and respectfully requests that this rejection be withdrawn.*" (see page 16 and 17 of the remarks). Although computer-readable storage medium encoded with instructions is known and typical in the art, these limitations must be included in the originally filed disclosure. Since the originally filed disclosure did not include computer-readable medium encoded with instructions, this limitation is seen as new matter. Furthermore, while page 7, lines 18-33 does disclose client software programmed onto user equipment, claims drawn to client side software at a user equipment would need to be clarified within the claims.

3. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 30, 32-34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to

one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claims 30, 32-34 recite the limitation "a computer readable storage medium". These limitations are not included in the applicant's originally filed disclosure (with respect to the 371 filing date), and therefore constitute new matter.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 19, 20, 41, and 42 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 19, 20, 41, and 42 are dependent on a cancelled claim. For the rejection, it is assumed that claims 19 and 20 depend on independent claim 12 and claims 41 and 42 depend on independent claim 37.

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1-5, 12, 13, 15, 16, 19-22, 26-30, 32-34, 37, 41-43, 47-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over BJELLAND et al (US 2002/0034935 A1) in view of the applicant's description of the prior art (hereinafter ADPA) and ALBERT et al (US 2003/0056096 A1).

Regarding claim 1, BJELLAND discloses a method (abstract), said method comprising: using an authentication message to signal a service selection information via a first network to an authentication server **[RADIUS]** of a second network, the service selection information indicating an access point (Figure 2, 3; paragraph 14, 15; mobile terminal request attachment to a network and context activation); and using said service selection information to connect to at least one service provided over said access point indicated by said service selection information (paragraph 15, 16; PDP context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would

have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 2, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said first network is a wireless local area network (ADPA - paragraph 4, 5; ALBERT – paragraph 3).

Regarding claim 3, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said second network is a cellular packet-switched network (BJELLAND – abstract; GPRS network; ADPA - paragraph 5, 6)

Regarding claim 4, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said cellular packet-switched network is a GPRS network (BJELLAND – abstract; GPRS network; ADPA - paragraph 5, 6).

Regarding claim 5, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said authentication message is an EAP message (ALBERT – paragraph 13, 57, 61).

Regarding claim 12, BJELLAND discloses an apparatus (abstract), comprising: a processor to extract from a received authentication message a service selection information to select a service (Figure 2, 3; paragraph 14, 15; mobile terminal request attachment to a network and context activation. It is noted that a processor and computing means would be inherently necessary for data extraction and processing), wherein the processor is configured to use said service selection information to establish a connection to services provided over an access point indicated by said service selection information (paragraph 15, 16; PDP context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 13, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said authentication message is an EAP message (ALBERT – paragraph 13, 57, 61).

Regarding claim 15, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said authentication server is a standalone WLAN authentication server (ALBERT – paragraph 55, 58).

Regarding claim 16, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said processor is a GPRS node (BJELLAND – abstract; GPRS network; ADPA - paragraph 5, 6).

Regarding claim 19, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA further discloses wherein at least one of said APN parameters is decrypted in said authentication server (ALBERT - paragraph 15-22, 64; furthermore, see independent claim regarding transmission and reception of data)

Regarding claim 20, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein at least one of said APN parameter is forwarded by the authentication server to said access point in an encrypted manner (ALBERT -

paragraph 15-22, 64; furthermore, see independent claim regarding transmission and reception of data).

Regarding claim 21, The combination of BJELLAND, ADPA, and ALBERT discloses a apparatus (abstract), comprising: a processor configured to set in an authentication message a service selection information regarding selection of a network service (paragraph 15, 16; PDP context activation. It is noted that a processor and computing means would be inherently necessary for data extraction and processing), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would

have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 22, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said authentication message is an EAP message (ALBERT – paragraph 13, 57, 61).

Regarding claim 26, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. BJELLAND further discloses wherein said service is a general packet radio service (abstract; paragraph 14-16).

Regarding claim 27, BJELLAND discloses a system [**Figures 1-3**] for providing access from a first network [**home network**] to a service of a second network [**external**

network], said system comprising: a terminal device configured to provide access to a network service, said terminal device configured to set in an authentication message a service selection information regarding selection of said network service (Figure 2, 3; paragraph 14, 15; mobile terminal request attachment to a network and context activation); and an authentication server device [**RADIUS server**] connected to a second network, said authentication server device configured for providing an authentication mechanism, said authentication server device configured to extract from a received authentication message said service selection information to select said service, and to use said service selection information to establish a connection to services provided over an access point indicated by said service selection information (paragraph 15, 16; PDP context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 28, BJELLAND discloses a method comprising: extracting, by a processor, from a received authentication message a service selection information to select a service (Figure 2, 3; paragraph 14, 15; mobile terminal request attachment to a network and context activation. It is noted that a processor and computing means is inherently necessary for data extraction and processing); and b) using, by a processor, said service selection information to establish a connection to services provided over an access point indicated by said service selection information (paragraph 15, 16; PDP context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 29, BJELLAND discloses a method comprising: setting in an authentication message a service selection information regarding selection of a network service at a terminal device (Figure 2, 3; paragraph 14, 15; mobile terminal request attachment to a network and context activation. It is noted that a processor and computing means is inherently necessary for data extraction and processing), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 30, BJELLAND discloses a computer-readable storage medium encoded with instructions configured to control a processor to perform a process (abstract; It is noted that a processor and computing means is inherently necessary for data extraction and processing), the process comprising: using an authentication message to signal a service selection information via a first network to an authentication server [**RADIUS**] of a second network, the service selection information indicating an access point (Figure 2, 3; paragraph 14, 15; mobile terminal request attachment to a network and context activation); and using said service selection information to connect to at least one service provided over said access point indicated by said service selection information (paragraph 15, 16; PDP context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 32, BJELLAND discloses a data structure embodied on a computer-readable medium (abstract), the data structure comprising: a service selection information to select a service (paragraph 15, 16; PDP context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 33, BJELLAND discloses a computer-readable storage medium encoded with instructions configured to control a processor to perform a process (abstract; it is noted that a processor and computing means would be inherently necessary to perform data extraction and processing), the process comprising: extracting from a received authentication message a service selection information to select a service (Figure 2, 3; paragraph 14, 15; mobile terminal request attachment to a network and context activation. It is noted that a processor and computing means would be inherently necessary for data extraction and processing), using said service selection information to establish a connection to services provided over an access point indicated by said service selection information (paragraph 15, 16; PDP context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would

have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 34, BJELLAND discloses a computer-readable storage medium encoded with instructions configured to control a processor to perform a process (abstract), the process comprising: setting in an authentication message a service selection information regarding selection of a network service (paragraph 15, 16; PDP context activation. It is noted that a processor and computing means would be inherently necessary for data extraction and processing), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 37, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said authentication message is an EAP message (ALBERT – paragraph 13, 57, 61).

Regarding claim 41, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. BJELLAND further discloses wherein at least one of said APN parameters is decrypted in said authentication server (ALBERT - paragraph 15-22, 64; furthermore, see independent claim regarding transmission and reception of data)

Regarding claim 42, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein at least one of said APN parameter is forwarded by the authentication server to said access point in an encrypted manner (ALBERT - paragraph 15-22, 64; furthermore, see independent claim regarding transmission and reception of data).

Regarding claim 43, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. The combination of BJELLAND, ADPA, and ALBERT further discloses wherein said authentication message is an EAP message (ALBERT – paragraph 13, 57, 61).

Regarding claim 47, see the rejections of the parent claim concerning the subject matter this claim is dependent upon. BJELLAND further discloses wherein said service is a general packet radio service (abstract; paragraph 14-16).

Regarding claim 48, BJELLAND discloses an apparatus (abstract), comprising: extracting means for extracting from a received authentication message a service selection information to select a service (Figure 2, 3; paragraph 14, 15; mobile terminal request attachment to a network and context activation. It is noted that a processor and computing means would be inherently necessary for data extraction and processing), controlling means for using said service selection information to establish a connection to services provided over an access point indicated by said service selection information (paragraph 15, 16; PDP context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Regarding claim 49, BJELLAND discloses an apparatus (abstract), comprising: setting means for setting in an authentication message a service selection information regarding selection of a network service (paragraph 15, 16; PDP context activation. It is noted that a processor and computing means would be inherently necessary for data extraction and processing), sending means for sending the authentication message (paragraph 15, 16; context activation), wherein said service selection information comprises at least one access point name parameter (paragraph 16; APN indicating relevant GGSN), wherein said at least one access point parameter comprises an access point name (paragraph 16), and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server (paragraph 16; DNS server used to read APN). However, BJELLAND does not expressly disclose wherein an access point parameter comprises a username and a password, and wherein the user name and password can only be decrypted at a network defined by the access point name. ADPA discloses wherein service selection information comprises at least one access point name parameter, wherein said at least one access point parameter comprises an access point name, a username and a password, and wherein said at least one access point name parameter is transmitted in said authentication message so that said access point name can be read by an access server, and the user name and password can only be read at a network defined by the access point name (paragraph 6 of the background of the invention). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify BJELLAND to include the teachings of ADPA, since ADPA states that such techniques were known and standard in the art (according to 3GPP TS 23.060) and therefore could be used to provide standardized protocol techniques to the existing invention. However, the combination of BJELLAND and ADPA does not expressly disclose the encryption and decryption of transmitted data. ALBERT discloses encryption and decryption of transmitted data (paragraph 15-22, 64). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combination of BJELLAND and ADPA to include the teachings of ALBERT, since ALBERT states that such a modification would allow a system to implement greater security measures when transmitting data (see paragraph 2, 64). Furthermore, the encryption and decryption of data along any two points of a network would increase data security between the two points.

Claim Rejections - 35 USC § 103

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 6, 7, 14, 23, 24, 38, 44, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over BJELLAND et al (US 2002/0034935 A1) in view of the applicant's description of the prior art (hereinafter ADPA) and ALBERT et al (US 2003/0056096 A1) and further in view of MCINTOSH et al (US 2003/0139180).

Regarding claim 6, 24, 45 see the rejections of the parent claim concerning the subject matter this claim is dependent upon. Although the combination of BJELLAND, ADPA, and ALBERT discloses the use of extensible authentication (EAP), the combination of BJELLAND, ADPA, and ALBERT does not expressly disclose wherein said extensible authentication protocol message is an extensible authentication protocol subscriber identity module or extensible authentication protocol authentication and key agreement message. In the same field of endeavor, MCINTOSH teaches wherein an extensible authentication protocol message is an extensible authentication protocol subscriber identity module or extensible authentication protocol authentication and key agreement message (paragraph 68, 71, 83, 92). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify O'NEILL to include the teachings of MCINTOSH, since such a modification would provide authentication means using a standardized protocol. Furthermore, the use of any known authentication means would have been an obvious design choice as any choice would provide secure network access.

Regarding claim 7, 14, 23, 38, and 44 see the rejections of the parent claim concerning the subject matter this claim is dependent upon. Although the combination of BJELLAND, ADPA, and ALBERT discloses the use of extensible authentication (EAP), the combination of BJELLAND, ADPA, and ALBERT does not expressly disclose wherein said authentication message is an EAP Challenge Response message. In the same field of endeavor, MCINTOSH discloses wherein an authentication message is an EAP Challenge Response message (paragraph 68, 71, 83, 121, 147). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify O'NEILL to include the teachings of MCINTOSH, since such a modification would provide authentication means using a standardized protocol. Furthermore, the use of any known authentication means would have been an obvious design choice as any choice would provide secure network access.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARIEL BALAOING whose telephone number is (571)272-7317. The examiner can normally be reached on Monday-Friday from 8:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, V. Paul Harper can be reached on (571) 272-7605. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VINCENT P. HARPER/
Supervisory Patent Examiner, Art Unit 2617

/Ariel Balaoing/
Examiner, Art Unit 2617

/A. B./
Examiner, Art Unit 2617